AO 106 (Rev. 06/09) Application for a Search Warrant

# UNITED STATES DISTRICT COURT

SEALED UNSEALED 2/4/15

for the

Southern District of California

FILED
2013 MAR 25 PM 1:56
CLERK U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

Google, Inc.
1600 Amphitheater Parkway, Mountain View, CA

Case No. 13 MJ8220

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 USC 2320; 18 USC 1956; 18 USC 1341; 18 USC 1343; 26 USC 7201; 26 USC 7206 | Trafficking of counterfeit goods and services; money laundering; mail fraud; wire fraud; tax evasion; and filing of false tax returns |

The application is based on these facts:

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Christiansen Madsen, SA ICE, HSI
*Printed name and title*

Sworn to before me and signed in my presence.

Date: 3-25-2013

*Judge's signature*

City and state: El Centro, CA

United States Magistrate Judge Peter C. Lewis
*Printed name and title*

1 kem

# ATTACHMENT A-3

## Place to Be Searched

Google, Inc. is an Internet Service Provider with its primary computer information systems and other electronic communications and storage systems, records and data located at 1600 Amphitheater Parkway, Mountain View, California 94043.

# ATTACHMENT B-3

## Particular Things to Be Seized

### I. Service of Warrant

The officer executing the warrant shall permit Google, Inc. ("the ISP"), as custodian of the computer files described in Section II below, to locate the files and copy them onto removable electronic storage media and deliver the same to the officer. The search of the data supplied by the ISP pursuant to this warrant will be conducted as provided in the "Procedures For Electronically Stored Information" of the affidavit submitted in support of this search warrant.

### II. Items Subject to Seizure

The items subject to seizure that will be found in the email account, **sumaliba@gmail.com**, from September 7, 2007 to the present, are **limited to**:

a. All subscriber and/or user information, including the name, address, and telephone number associated with the account, histories, buddy lists, profiles, method of payment, detailed billing records, access logs, transactional data and any other files associated with this account and related screen names;

b. Communications and attachments related to the purchase, sale, and shipment of counterfeit cellular phone parts, accessories, batteries for electronic devices, and other electronics;

c. Communications and attachments related to bank accounts and other financial information;

d. Communications and attachments related to receipt of income, expenditures, and acquiring or selling assets;

**Which evidence:** (1) trafficking in counterfeit goods and services ((18 U.S.C. § 2320), (2) money laundering (18 U.S.C. § 1956), (3) mail fraud (18 U.S.C. § 1341), (4) wire fraud (18 U.S.C. § 1343), (5) tax evasion (26 U.S.C. 7201), and (6) filing false returns (26 U.S.C. § 7206(1)), relating to

the purchase and shipment of counterfeit cellular phone parts and other electronics from China to the United States, the resale of such counterfeit parts in the United States and elsewhere, and the receipt and distribution of payments for such parts.

# AFFIDAVIT

I, Christiansen C. Madsen, being duly sworn, state as follows:

## I. INTRODUCTION

### A. Training and Experience

1. I am a Special Agent with the U.S. Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations with the Department of Homeland Security. I have been so employed since January 3, 2010. Prior to my employment with ICE, I served as a United States Secret Service Uniformed Division Officer from October 2004 to January 2010.

2. I am a graduate of the Federal Law Enforcement Training Center ("FLETC"). At FLETC, I received training in criminal investigative techniques, including financial investigations, the execution of search warrants, and other areas of law enforcement. Since becoming an agent, I have also received both formal and on-the-job training in the laws and regulations relating to the trafficking of counterfeit goods and services, money laundering, mail fraud, and wire fraud. I have also directed, and participated in, numerous investigations that involved these crimes. Additionally, I have led and/or participated in dozens of search warrants, including several electronic search warrants that targeted commercial fraud. I also communicate regularly with investigators with expertise in computers, computer forensics, and internet-based investigations. As a federal agent, I am authorized to investigate violations of laws of the United States and I

am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

**B. Purpose of This Affidavit**

3. This affidavit is made in support of applications for search warrants for the below-listed Internet Service Providers ("ISP") and respective email accounts:

a. Microsoft, Inc. ("Microsoft"), 1065 La Avenida, Mountain View, California 94043 (described in Attachments A-1, A-2) for the following email accounts:

**duhongwei88@hotmail.com** (described in Attachment B-1); and

**amcellular@hotmail.com** (described in Attachment B-2).

b. Google, Inc. ("Google"), 1600 Amphitheater Way, Mountain View, California 94043 (described in Attachment A-3) for the following email account:

**sumaliba@gmail.com** (described in Attachment B-3).

c. GoDaddy, Inc. ("GoDaddy"), 14455 North Hayden Road, Suite 219, Scottsdale, Arizona 85260 (described in Attachment A-4) for the following email account:

**sales@ocesa.com** (described in Attachment B-4).

4. The statements in this affidavit are based on my training and experience, my personal knowledge, my participation in other federal investigations, my conversations with other law enforcement agents and third parties, and my review of records obtained during this investigation. Because this affidavit is submitted for the limited purpose of

securing the search warrants as described herein, it does not include every fact known to me concerning the investigation. I set forth only the facts necessary to establish that probable cause exists to believe that evidence of trafficking of counterfeit goods and services (18 U.S.C. § 2320), money laundering (18 U.S.C. § 1956), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), tax evasion (26 U.S.C. § 7201), and filing of false returns (26 U.S.C. § 7206(1)) (more particularly described in Attachments B-1 through B-4) will be located within the servers and records of the ISPs listed above (more particularly described in Attachments A-1 through A-4). It is my opinion that such probable cause exists based on the information set forth below.

## II. PROBABLE CAUSE

### A. Background

5. In March 2012, Apple, Inc. ("Apple") notified law enforcement that the website flexqueen.com was possibly trafficking in counterfeit goods. Based on a variety of investigative measures that include seizures of counterfeit goods from Flexqueen, agents have determined that Flexqueen sells counterfeit cellular phone parts and other electronics to customers in the United States and abroad primarily through its website. Sales records indicate that Flexqueen purchases the counterfeit goods from a Chinese supplier. Payment records indicate Flexqueen averages well over $1,000,000 in online sales alone. Thus far, agents have not identified any authentic items sold by Flexqueen.

6. Based on records related to purchases of counterfeit items from

flexqueen.com by an undercover agent and investigators from Apple, agents have determined that Flexqueen and Ocesa Manufacturing are the same entity. For example, Apple received a bill from "Flexqueen/Ocesa Manufacturing" after it purchased a counterfeit Apple part through the flexqueen.com website. The same email revealed that Ocesa Manufacturing operates a second website, ocesa.com, which also sells cellular phone parts and other electronics-related items.

7. In November 2012, agents executed a court-authorized search warrant of flexqueen.com and its attendant email accounts. Although agents have not yet received all information subject to the search warrant, records received to date reveal that: (1) the website was started on September 7, 2007; (2) it is registered to Yolanda Martinez, with Ricardo Puente as the listed registrant for the PayPal account linked to Flexqueen.com for payment processing; (3) Puente runs a Flexqueen-affiliated store in Mexico; (4) the target email accounts listed above are used by those running flexqueen.com and other coconspirators in furtherance of their criminal activity; (5) the accounts **duhongwei88@hotmail.com** and **sumaliba@gmail.com** are used by an individual (believed to be a Chinese national named Hongwei Du, aka "Nick Du") who supplies Flexqueen with counterfeit goods; and (6) the accounts **amcellular@hotmail.com** and **sales@ocesa.com**, are email accounts used by the self-described owner of Flexqueen, Octavio Sana ("Sana"), and other Flexqueen personnel.

8. A records check for ocesa.com revealed that its website administrator is

"Abel Sana." Law enforcement database checks show that Abel Sana is associated with 1248 E. Calle De Oro, Calexico, California. California Department of Motor Vehicles ("DMV") records list this address as the residence for Octavio Sana. Sana was the listed consignee (i.e., ultimate recipient) on numerous importations of electronics from China from January 2012 through February 2013 that were shipped to Flexqueen/Ocesa Manufacturing at 1356 Truman Court, Calexico, California and his storefront located at 656 9th Avenue, San Diego, California. Surveillance has identified 1356 Truman Court, Calexico, California as Flexqueen's main address, although employees have referenced other locations like the store operated by Puente, in emails. Agents have seen stacked boxes that nearly fill the entire two-car garage of the Truman residence and have observed individuals make what appear to be daily mail runs to local post offices. And, in a letter attached to an email found pursuant to the November search, Sana identified himself as the owner of flexqueen.com. The letter, dated November 28, 2012, appears to have been a reference for Petra Ramirez Yolanda Lerma (aka "Yolanda Martinez"), a Flexqueen employee and coconspirator who, based on Sana's letter, works at Flexqueen's "Mexicali, BC, Mexico" office.

9. Emails indicate that Saduan Electronic, Du's company, is Flexqueen's primary – and possibly sole – source for counterfeit goods. United States Customs' records, however, show that Flexqueen and Sana received cell phone parts and other electronics from approximately 50 Chinese exporters from January 2012 to February

2013, including Saduan. Emails indicate that in addition to directly shipping counterfeit goods to Flexqueen, Saduan utilizes third-party exporters as well. A review of law enforcement databases revealed that United States law enforcement has seized a variety of counterfeit goods (e.g., electronics, dvds, personal care items, tax-exempt cigarettes) shipped by approximately 28 of the companies that have exported electronics from China to Flexqueen.

10. Agents have also conducted multiple undercover purchases of several products that were subsequently confirmed as counterfeit items. In May 2012, agents purchased a number of items from flexqueen.com that purported to be Apple iPhone parts (they were all marked with either the Apple logo or the word "APPLE"). After the purchases, Apple determined that the purchased items were counterfeit. And on June 1, 2012, an undercover agent ("UC-1") contacted Flexqueen and posed as a potential buyer of large quantities of counterfeit cell phone parts. Agents recorded conversations UC-1 had with Flexqueen employee, Angela Vela. During the conversations, Vela acknowledged that Flexqueen sold counterfeit parts. For example, in response to UC-1 statement that Flexqueen sold high quality counterfeit parts, Vela responded, "Yeah." And when UC-1 told Vela that one of Flexqueen's products looked "exactly like it came from Apple," Vela responded, "Right." Vela later told UC-1 that Flexqueen had iPhone 4S kits (the external covers for the iPhone 4S phone) "in all different types of colors." Vela continued, "No, I don't think they [Apple] have this many, or this variety of colors."

Apple confirmed that legitimate iPhone 4S kits only come in white or black. Vela also quoted UC-1 prices for different items and offered that if they did the deal in person, UC-1 "can, like, not worry about tax and shipping and all that." UC-1 eventually agreed to buy 250 iPhone digitizer screens. When they met to complete the deal, Vela explained, "The only thing that will get you in trouble on that is the actual Apple logo on the back." Vela told UC-1 that the shipment should be available the following week, as it was arriving from "Asia."

11. On July 10, 2012, agents identified the suspected shipment that Vela referenced at the Los Angeles International Airport. The shipment was from Saduan Electronic (Du's company) and intended for the "Imperial Valley Trading Company" at Flexqueen's Truman Court address in Calexico. Agents seized approximately 600 electronics parts, including 345 LCD digitizer screens that purported to be manufactured by Apple (the word "APPLE" was stamped on a cable attached to the screens) pursuant to a search of the Saduan shipment. Apple confirmed that the digitizer screens were counterfeit. A Customs and Border Protection ("CBP") importations expert estimated the retail value of the items, if legitimate, to be approximately $187,498.

12. Following the seizure, on July 12, 2012, Vela emailed Sana at his **amcellular@hotmail.com** address: "DHL Package [sic] that is being held, is still being held, no additional information is needed. They will email me with more additional information tomorrow. I have already contacted [Undercover Agent's alias] concerning

this, but no answer back from him yet." Sana appears to be the principal user of the **amcellular@hotmail.com** account for a couple reasons. First, the email from Vela was copied to "octaviocesarsana@gmail.com." Second, in other emails discovered pursuant to the November 2012 search warrant, emails to the **amcellular@hotmail.com** are addressed to "Octavio." GoDaddy Inc., the ISP for the website, saduan.com, indicates that Sana registered the website and listed **amcellular@hotmail.com** as the related email account and the 1248 E. Calle De Oro, Calexico residence as the billing address.

13. As noted above, Flexqueen operates multiple locations in addition to its Calexico address. Email records indicate they maintain at least one location in Mexico and agents have observed Sana operating a store front in downtown San Diego called SD Cell Repair. For example, on September 11, 2012, a plain-clothes agent inquired with Sana at SD Cell Repair about the cost to repair a screen for a Samsung Epic Galaxy cell phone. The agent observed Sana look up the item's price on flexqueen.com. The agent then asked Sana about iPhone LCD screens and back covers, which were marked with the Apple logo, in an assortment of colors such as pink, green, purple, and red. When the agent asked Sana how he had "iPhone" covers in these colors when Apple only makes them in black and white, Sana replied that the covers were "generic, not original." Sana also told the agent he had a replacement battery for a Samsung Epic cell phone available for $10 because it too was "generic," not original. Sana showed the agent a replacement battery and remarked that it looked exactly like an original battery. The agent purchased

the battery for $10. Sana did not provide the agent with a receipt. Inspection of the battery revealed the word "Samsung" printed on the exterior of the battery. Samsung later confirmed that the battery purchased by the agent on September 11, 2012 from Sana's SD Cell Repair location was counterfeit.

**B. Sana, Du and Other Target Subjects Use the Target Email Addresses In Furtherance of Their Scheme to Sell Counterfeit Goods**

(1) **duhongwei88@hotmail.com**

14. Du corresponds with Sana and other Flexqueen employees about the sale and distribution of counterfeit cell phone parts and other electronics using the email account, **duhongwei88@hotmail.com**. For instance, from March 23, 2012 to August 20, 2012, he used this account to correspond with Flexqueen personnel approximately 47 times.

15. In several emails, Du discussed with Flexqueen personnel flaws in the counterfeit items he sent them:

a. On April 18, 2012, "Angela" (believed to be Angela Vela, using the admin@flexqueen.com email address) emailed Du at **duhongwei88@hotmail.com** to address concerns with the quality of some items Flexqueen had recently received from Saduan. Specifically, Vela pointed out an inconsistency with one product. She wrote Du, "[W]e have two different types of Huawei M865 digitizers, one is longer than the other, and the top notch is longer on the long digitizer." Vela attached pictures of the two versions of the same digitizer screen to illustrate the differences between the two. The

manufacturer, Huawei, has not responded to law enforcement's inquiries about the authenticity of the product discussed by Du and Vela. Nonetheless, based on my training and experience, as well as my knowledge of this case, I believe the digitizers purported to be authentic Huawei parts are, in fact, counterfeit. In my experience, the manufacturers of authentic parts do not make "different types" of the same part. Furthermore, I have yet to find a legitimate manufacturer who sells such parts independently. Rather, they only sell them as a completed unit.

b. On May 17, 2012, "Yolanda M." (believed to be Petra Yolanda Lerma Ramirez) emailed Du at **duhongwei88@hotmail.com** from Flexqueen's admin@flexqueen.com email address. The screen name associated with Flexqueen's admin@flexqueen.com email address is "Yolanda Martinez." Martinez told Du, "Mytouch 3G housing with NO audio hole. Please see images below from a customer. All our housings are pretty much the same." The attached pictures show the inside and outside of two different versions of the Mytouch 3G external casing. Based on a review of the pictures, the two versions appear to be the same basic component, but with many subtle differences (e.g., missing pieces, different sized openings).[1]

c. On June 12, 2012, "Angela" emailed Du at **duhongwei88@hotmail.com** from the admin@flexqueen.com email address to notify

[1] Because of the poor quality of the picture, T-Mobile was not able to tell whether these parts were authentic or counterfeit from only reviewing the photographs. T-Mobile confirmed, however, that Saduan Electronic is not an authorized supplier of T-Mobile parts.

him of missing parts in HTC Sensation 4G mainboards (the main "computer" in the phone). Vela wrote, "The HTC Sensation 4G mainboard flex cables seem to be having some problems. They are missing some parts." Vela attached a picture of a complete mainboard and a picture of a mainboard that was missing certain parts. A review of the pictures confirms that parts appear to be missing in one version of the mainboard. HTC did not respond to agents' inquiries about the authenticity of the parts discussed in Vela's email. Nonetheless, based on my training and experience, I believe the parts are counterfeit because of the inconsistency of components between what should be identical HTC Sensation 4G mainboards.

c. On June 25, 2012, "Angela" emailed Du at **duhongwei88@hotmail.com** from the admin@flexqueen.com email address a photograph of two iPod 4th generation LCD Digitizers (the touch-screen portion of an iPod). Superimposed over a portion of the photograph is Flexqueen's description of a flaw in the LCD digitizer screen previously delivered by Saduan. Specifically, Vela addressed several new and prior complaints to Du in the email: (1) "The Blackberry 9800 cam sliding flexes [sic] have been getting returned by customers, they are saying the [sic] are cracked for [sic] ripped in parts. The generic version [counterfeit] appears to be missing a part . . .;" (2) "The most recent order of Blackberry 8350i Royal Blue houses that arrived are shinier and darker in color, and very nice, much better than the last ones we had;" and (3) "Last shipment of iphone [sic] 4 GSM LCD + Digitizer in White; they

came in more grayish than white (customer complained about this). We need a brighter light color like what used to come in before." Elsewhere in the email, Vela let Du know that Sana was aware of the issues with Saduan's products. "Ocatvio asks that you be more careful and inspect the merchandise more." Apple later reported that it does not manufacture or sell iPhone parts separately. Thus, the very nature that Flexqueen obtained the individual parts from Saduan indicates that they are counterfeit.

16. Du has also used the **duhongwei88@hotmail.com** address to offer Flexqueen personnel new counterfeit items. On April 3, 2012, Du emailed Sana the price and several pictures of various protective cases for iPhones (including some with the Apple logo) at Sana's **amcellular@hotmail.com** (in the version obtained by agents, the "To" line of Du's email is a hyperlink for "amcellular"). Later that day, Du forwarded the same email to Vela at support@flexqueen.com, telling her that "Octavio asked me about you [sic] for this . . ." Based on Du's email to Vela, I believe that Du and Sana communicated either through another means (e.g., internet video conferencing like Skype) or through alternate email addresses because there is no record of further communication about these new products on either Sana's **amcellular@hotmail.com** account or Du's **duhongwei88@hotmail.com** account. Vela responded to Du, "Are these supposed to be some sort of protective case? How does the iPhone fit in there without falling?" Apple has confirmed that the protective cases pictured in the April 3, 2012 email are indeed counterfeit. Apple further stated that it does not authorize these

protective cases to be manufactured independently.

(2) **Sumaliba@gmail.com**

17. Beginning around the time of the July 10, 2012 seizure of over 600 counterfeit cell phone parts, Vela and others at Flexqueen traded several emails with Du over his **sumaliba@gmail.com** email address. In fact, from June 26, 2012 to November 7, 2012, Du used the **sumaliba@gmail.com** email address approximately 10 times to communicate with Flexqueen email addresses. For instance, in an August 16, 2012 email about the July 10 seizure, Du explained to Vela that only the "branded" items, meaning those items with identifiable, counterfeited, trademarks, were seized. Du further told Vela that Flexqueen should have received the remainder of the "unbranded" shipment, meaning those items with no identifiable trademarks. In fact, CBP seized the items with trademarks on them but allowed those items with no commercial markings to be delivered.

18. On November 6, 2012, Vela sent Du an order to the **sumaliba@gmail.com** account. She provided Du with general information about products Flexqueen needed, including some parts that are obviously counterfeit (e.g., "iPhone 4 GSM Pink Kits") – again, Apple does not make such kits in any colors other than black or white.

19. The emails from Vela to Du's **sumaliba@gmail.com** also indicated that Sana does, in fact, maintain a leadership role with Flexqueen. While Vela provided Du with a general list of items Flexqueen needed, she instructed Du to follow up with Sana

about the specifics of Flexqueen's order. She wrote, "[P]lease confirm with Octavio first on things we need." Subsequent emails between Vela and Du indicated that Du was trying to reach Sana via the online video chat provider, Skype. Vela told Du that Sana "replies when he can." She promised that she would contact Sana to let him know that Du was attempting to reach him.

(3) **amcellular@hotmail.com**

20. The **amcellular@hotmail.com** account is one of five email addresses listed for Flexqueen's PayPal account, which processes a substantial portion of its online sales. Flexqueen's PayPal account is under Puente's name. We know that Flexqueen uses the PayPal account for its counterfeit sales. In February 2012, Apple investigators purchased through PayPal items that Flexqueen purported to be Apple products, and in May 2012, UC-1 did the same. All products purchased Apple and UC-1 were determined to be counterfeit by Apple.

21. Email records obtained from the November 2012 search indicate that Sana uses the email address, **amcellular@hotmail.com**, to communicate with Du about Flexqueen's purchase and sale of counterfeit goods. For example, on a May 8, 2012 email, Du (using the **duhongwei88@hotmail.com** account) provided Sana with the "PI" (purchase invoice) and tracking number for a recent shipment. Sana's use of the **amcellular@hotmail.com** account is illustrated by the fact that Du addressed the email, "Hi Octavio." Flexqueen email records also reflect that Du uses his

**sumaliba@gmail.com** account to communicate with Sana at **amcellular@hotmail.com** as well. For example, on July 19, 2012, Du emailed Vela and Sana (**amcellular@hotmail.com**) to inform them that he had recently received new "BB 9800 Dig," meaning Blackberry 9800 digitizers. Du also informed Sana and Vela that they received "3 unit defectives [sic] and 1 missing!!" Du appears to have been telling Vela and Sana that three units he received had defective parts and that he did not receive one unit that he had ordered. Du's reference to having received defective parts indicates two things: (1) the parts he is referring to are counterfeit; and (2) Saduan may not be the ultimate manufacturer of the counterfeit goods. Finally, the November 2012 search revealed that Sana receives invoices of transactions to his **amcellular@hotmail.com** account. For instance, on August 15, 2012, Du emailed Vela and Sana (**amcellular@hotmail.com**) the "commercial invoice" for a recent shipment that he said was "for ur [sic] check." Emails and Customs records suggest that Du provides Flexqueen with two sets of invoices – one that accompanies the actual package through Customs inspection and a second that he sends to them directly via email. In my training and experience, I know that international counterfeiters will use "double invoicing" as a means of avoiding the full duties owed to Customs on imported items. The invoice that accompanies the shipment reflects a drastically reduced value of goods versus what the goods are actually worth. The distributor will then provide the buyer with a second invoice, again, in an email like this, which reflects the actual terms of the deal.

22. The November 2012 email search also revealed that Sana used **amcellular@hotmail.com** to communicate with other Flexqueen personnel almost 300 times from July 7, 2009 to November 7, 2012. Examples include:

a. On August 8, 2012, Sana sent an email from **amcellular@hotmail.com** to **yolanda@flexqueen.com** with a subject of "RE: Rv: Precios faltantes para Mario [meaning, 'Missing prices for Mario']."[2] Sana's email listed prices for a number of products, including one described as "Kit del Iphone 4s de colores [meaning, 'Kit color Iphone 4s']," with a corresponding prices of $49.99 and $37.50. The second price appeared to be a discounted price for "Mario." Again, Apple does not manufacture this component in any other colors but black and white, which suggests that this price list references counterfeit Apple products. This conclusion is corroborated by the fact that the suggested retail price for an authentic Apple iPhone 4 "kit" costs $140.

b. On September 4, 2012, Martinez sent two separate emails from yolanda.lerma@hotmail.com to **amcellular@hotmail.com**. The subject line of one email was "Frentes Torch [meaning, 'Fronts Torch']. Two photographs attached to the email appeared to be the front and back of a black LCD screen for a Blackberry Torch cell phone. The second email, whose subject line read, "FW: Frentes blancos [meaning, 'White Fronts']," had attached two photos of the front and back of a white LCD screen of a Blackberry Torch cell phone. Research in Motion ("RIM"), the manufacturer of

[2] I consulted with Spanish-speaking law enforcement personnel on all translations contained in this affidavit.

Blackberry products, could not determine whether the products were authentic or not due to the poor quality of the pictures. RIM stated, however, that like Apple, it does not manufacture or sell parts separately for sale on the aftermarket.

c. On September 20, 2012, Vela emailed (**admin@flexqueen.com**) Sana (**amcellular@hotmail.com** and **octaviocesarsana@gmail.com**) about a recently received package. Vela wrote, "Also these are the rest of the items that came in Shirleys [sic] package today. They are LCD+DIGITIZERS for the COMPLETE KITS but none of the battery doors came in like [sic] in the previous box. iPhone 4 GSM: MIRROR PURPLE – 15." Vela provided the other contents of the package: "iPhone 4S: MIRROR ORANGE – 12 MIRROR GOLD – 12 DARK BLUE – 12 LIGHT BLUE – 8 ARMY CAMO BLUE – 9 ARMY CAMO GREEN – 3." Again, because Apple only produces these items in white or black, the parts referenced in this email were almost certainly counterfeit. Moreover, these "kits" are likely the same as the ones purchased by an UC-1 on May 29, 2012, which were determined to be counterfeit.[3]

23. Finally, it is worth noting that while agents have discovered several instances of Sana's use of **amcellular@hotmail.com** to carry out the scheme, agents believe the requested warrant is necessary to get a more complete picture of Sana's use of this account. Because the November 2012 search only revealed emails to **amcellular@hotmail.com** when it was copied on another email subject to the November

[3] On February 21, 2013, Vela (admin@flexqueen.com) wrote UC-1, "The kits for the iphone come in camo green & camo sky blue."

2012 search, agents believe Sana uses it far more extensively than what was revealed in November 2012.

(4) **sales@ocesa.com**

24. The email address, **sales@ocesa.com**, is Flexqueen's primary email address for its PayPal account. In fact, records indicate that customer payments through PayPal are routed through the **sales@ocesa.com** email account. PayPal records indicate $4,387,090.34 have been processed through **sales@ocesa.com** since the Flexqueen account was opened approximately four years ago. And from January 1, 2012 to June 7, 2012, records reflected $489,168.07 in sales through the PayPal account. During the same general time frame, January 3, 2012 and June 4, 2012, Flexqueen made 37 transfers from the PayPal account to an Ocesa Manufacturing financial account for a total of $375,940.00. Again, based on a variety of sources, including statements Vela made to UC-1, Ocesa Manufacturing is essentially Flexqueen's alter ego. These transfers correlate to wire transactions from Ocesa to Saduan, the supplier of counterfeit cell phone and other electronics parts to Flexqueen. For example, PayPal records indicate that three transfers were made to the Ocesa account on January 3, 4, and 6, 2012, in the total amount of $29,350. Bank records further show a wire transfer of $28,267.73 from Ocesa's account to Saduan on January 6, 2012. And on January 19, 24 and 30, 2012, three more transfers were made from Flexqueen's PayPal account (**sales@ocesa.com**) to the same Ocesa account that totaled $40,350. On January 31, 2012, Ocesa once again

transferred a commensurate amount -- $32,517.73 -- to Saduan. Records show similar activity in the PayPal account in 2011: a total of $1,580,477.18 was transferred from the PayPal account to the Ocesa business account over 140 transactions. Based on the above, I believe there is probable cause that **sales@ocesa.com** contains payment records and written communications between Sana and other Flexqueen personnel and Flexqueen's customers regarding the sales of counterfeit items.

25. Finally, the November 2012 email search did reveal evidence that Flexqueen uses **sales@ocesa.com** to communicate about its counterfeit trafficking business as well. For instance, on October 19, 2012, Martinez emailed **sales@ocesa.com** and yoland@flexqueen.com a prior email she had sent Sana about an apparent order from a customer. Specifically, the order contained several items Apple has said it does not make, including iPhone 4 kits in red and "rose."

### C. Target Subjects' Retention of Emails

26. Based on my training and experience, I know that individuals who utilize emails in furtherance of their criminal activities tend to retain the emails in their accounts for a long period of time. This is particularly true of individuals involved in commercial fraud, like here. As explained above, Flexqueen and Saduan rely on their email communications to buy and sell counterfeit electronics parts. The previous email search revealed several invoices sent and received over relevant Flexqueen and Saduan email accounts as well. Because of how they use email, it is common for them to retain the

emails of their commercial transactions for a long period of time in order to maintain a record of any given transaction. In fact, the November 2012 search revealed some emails as old as 47 months. Moreover, the emails obtained to date indicate that Flexqueen and Saduan personnel have little fear of their email traffic being discovered by law enforcement (thus, little cause for them to delete such communications). For instance, after the July 10, 2012 seizure of 600 counterfeit cell phone parts, not only did Du communicate with Flexqueen over his **sumaliba@gmail.com** account about the seizure, but also about other orders as well. And the same was true for Vela's use of the **admin@flexqueen.com** account. Thus, not only is email critical to their fraudulent scheme, but they are, apparently, operating with little fear of law enforcement detection of their email. These factors, along with my training and experience, cause me to believe that the users of the target email accounts will retain relevant emails in the accounts for long periods of time.

## III. THE INTERNET SERVICE PROVIDERS

27. Microsoft, Inc., Google, Inc., and GoDaddy, Inc. are ISPs that, among other things, provides electronic communication services to subscribers. The ISPs' electronic mail services allow subscribers to communicate with other subscribers and with others through the Internet. The ISPs' subscribers access subscriber services through the Internet.

28. The ISPs' subscribers use screen names during communications with others. The screen names may or may not identify the real name of the person using a particular screen name.

29. At the creation of an account with the ISP and for each subsequent access to the account, the ISP typically logs the Internet Protocol (IP) address of the computer accessing the account. An IP address is a unique address through which a computer connects to the Internet. IP addresses are leased to businesses and individuals by ISPs. Obtaining the IP addresses that have accessed a particular ISP account often identifies the ISP that owns and has leased that address to its customer. Subscriber information for that customer then can be obtained using appropriate legal process.

## IV. PROCEDURES FOR ELECTRONICALLY-STORED INFORMATION

30. Federal agents and investigative support personnel are trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of the ISPs are not. It would be inappropriate and impractical for federal agents to search the vast computer network of the ISPs for the relevant accounts and then to analyze the contents of those accounts on the ISPs' premises. The impact on the ISPs' business would be severe.

31. Therefore, I request authority to seize all content, including electronic mail and attachments, stored instant messages, stored voice messages, photographs and any other content from the ISPs' accounts, as described in Attachment B-1 – B-4. In order to

accomplish the objectives of the search warrants with a minimum of interference with the business activities of the ISPs, to protect the rights of the subject(s) of the investigation and to effectively pursue this investigation, authority is sought to allow the ISPs to make digital copies of the entire contents of the accounts subject to seizure. Those copies will be provided to me or to any authorized federal agent. The copies will be forensically imaged and the image will then be analyzed to identify communications and other data subject to seizure pursuant to Attachment B-1 – B-4. Relevant data will be copied to separate media. The original media will be sealed and maintained to establish authenticity, if necessary.

32. Analyzing the data to be provided by the ISPs may require special technical skills, equipment and software. It also can be very time-consuming. Searching by keywords, for example, often yields many thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrants. Merely finding a relevant hit does not end the review process. Certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications, which files may have been attached to electronic mail, do not store data as searchable text. The data is saved in a proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases dramatically.

33. Based on the foregoing, searching the recovered data for the information subject to seizure pursuant to these warrants may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained. The personnel conducting the examination will complete the analysis within ninety (90) days of receipt of the data from the service provider, absent further application to this court.

34. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize all electronic mails that identify any users of the subject accounts and any electronic mails sent or received in temporal proximity to incriminating electronic mails that provide context to the incriminating mails.

35. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of these warrants.

## V. REQUEST FOR SEALING AND PRECLUSION OF NOTICE

36. This is an ongoing investigation of which the target(s) is unaware. It is very likely, based upon the above, that evidence of the crimes under investigation exists on ISPs' server space subject to the control of the target. There is reason to believe, based on the above, that premature disclosure of the existence of the warrants will result in destruction or tampering with that evidence and seriously jeopardize the success of the

investigation. Accordingly, it is requested that the warrants and all related materials be sealed until further order of the Court. In addition, pursuant to Title 18, United States Code, Section 2705(b), it is requested that this Court order the ISPs to whom this warrant is directed not to notify anyone of the existence of the warrants, other than its personnel essential to compliance with the execution of these warrants until further order of the Court.

## VI. CONCLUSION

37. Based on the foregoing, I believe probable cause exists to believe that the items in Attachments B-1 through B-4 constitute evidence of violations of Title 18, U.S.C. § 2320 (trafficking of counterfeit goods and services), Title 18 U.S.C. § 1956 (money laundering), Title 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. §1343 (wire fraud), Title 26 U.S.C. § 7201 (tax evasion) and Title 26 U.S.C. § 7206(1) (filing of false returns), and that such items will be found at the locations to be searched as described in Attachments A-1 through A-4.

Christiansen Madsen, Special Agent
Homeland Security Investigations

Subscribed to and sworn before me on this 25th day of March , 2013.

HONORABLE PETER C. LEWIS
United States Magistrate Judge